

1
2
3
4
5
6
7 **UNITED STATES DISTRICT COURT**
8 **WESTERN DISTRICT OF WASHINGTON**

9 STRIKE 3 HOLDINGS, LLC, a Delaware
10 corporation,

11 Plaintiff,

12 vs.

13 JOHN DOE subscriber assigned IP address
73.225.38.130,

14 Defendant.
15

Case No.: 2:17-cv-01731-TSZ

**FIRST AMENDED COMPLAINT FOR
COPYRIGHT INFRINGEMENT**

JURY DEMAND

16 Plaintiff, Strike 3 Holdings, LLC, by and through its undersigned counsel, alleges for its
17 First Amended Complaint against John Doe subscriber assigned IP address 73.225.38.130 as
18 follows:

19 **Introduction**

20 1. This case is about ongoing and wholesale copyright infringement of Plaintiff's
21 motion pictures by Defendant, who can only be identified by an IP address.

22 2. Plaintiff, Strike 3 Holdings, LLC ("Strike 3" or "Plaintiff"), is the owner of
23 award winning, critically acclaimed adult motion pictures.

24 3. Strike 3's motion pictures are distributed through the *Blacked*, *Tushy*, *Vixen*, and
25 *Blacked Raw* adult websites and DVDs. With more than 20 million unique visitors to its
26

27 FIRST AMENDED COMPLAINT
28 (Case No.: 2:17-cv-01731-TSZ)

FOX ROTHSCHILD LLP
1001 Fourth Avenue, Suite 4500
Seattle, WA 98154
(206) 624-3600

1 websites each month, the brands are famous for redefining adult content, creating high-end,
 2 artistic, and performer-inspiring motion pictures produced with a Hollywood style budget and
 3 quality.

4 4. Defendant is, in short, stealing these works on a grand scale. Using the
 5 BitTorrent protocol, Defendant is committing rampant and wholesale copyright infringement by
 6 downloading Strike 3's motion pictures as well as distributing them to others. Defendant did
 7 not infringe just one or two of Strike 3's motion pictures, but has been recorded infringing
 8 eighty-seven movies over an extended period of time.

9 5. Although Defendant attempted to hide this theft by infringing Plaintiff's content
 10 anonymously, Defendant's Internet Service Provider ("ISP"), Comcast Cable Communications,
 11 LLC has identified Defendant through his or her IP address 73.225.38.130.

12 6. This is a civil action seeking damages under the United States Copyright Act of
 13 1976, as amended, 17 U.S.C. §§ 101 et seq. (the "Copyright Act").

14 **Jurisdiction and Venue**

15 7. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C.
 16 § 1331 (federal question); and 28 U.S.C. § 1338 (jurisdiction over copyright actions).

17 8. This Court has personal jurisdiction over Defendant because Defendant used an
 18 Internet Protocol address ("IP address") traced to a physical address located within this District
 19 to commit copyright infringement. Therefore (i) Defendant committed the tortious conduct
 20 alleged in this first amended complaint in this State; (ii) Defendant resides in this State and/or;
 21 (iii) Defendant has engaged in substantial – and not isolated – business activity in this State.

22 9. Plaintiff used IP address geolocation mapping by Maxmind Inc. ("Maxmind"),
 23 an industry-leading provider of IP address intelligence and online fraud detection tools, to
 24 determine that Defendant's IP address traced to a physical address in this District. Over 5,000
 25 companies, along with United States federal and state law enforcement, use Maxmind's GeoIP

1 data to locate Internet visitors, perform analytics, enforce digital rights, and efficiently route
2 Internet traffic.

3 10. Although Defendant is only known to Plaintiff by his or her IP Address, the
4 Court possesses the true name and physical address of the Defendant and can confirm he or she
5 resides within the Western District of Washington.

6 11. Pursuant to 28 U.S.C. § 1391(b) and (c), venue is proper in this district because:
7 (i) a substantial part of the events or omissions giving rise to the claims occurred in this District;
8 and, (ii) the Defendant resides (and therefore can be found) in this District and resides in this
9 State. Additionally, venue is proper in this District pursuant 28 U.S.C. § 1400(a) (venue for
10 copyright cases) because Defendant or Defendant's agent resides or may be found in this
11 District.

12 **Parties**

13 12. Strike 3 is a Delaware limited liability company located at 2140 S. Dupont Hwy,
14 Camden, DE.

15 13. Plaintiff currently can only identify Defendant by his or her IP address.
16 Defendant's IP address is 73.225.38.130. Defendant's Internet Service Provider has provided
17 Defendant's name and address to the Court.

18 **Factual Background**

19 ***Plaintiff's Award-Winning Copyrights***

20 14. Strike 3's subscription based websites proudly boast a paid subscriber base that
21 is one of the highest of any adult-content sites in the world. Strike 3 also licenses its motion
22 pictures to popular broadcasters and Strike 3's motion pictures are the number one selling adult
23 DVDs in the United States.

24 15. Strike 3's motion pictures and websites have won numerous awards, such as
25 "best cinematography," "best new studio," and "adult site of the year." One of Strike 3's
26 owners, three-time director of the year Greg Lansky, has been dubbed the adult film industry's

1 “answer to Steven Spielberg.”

2
3 16. Strike 3’s motion pictures have had positive global impact, leading more adult
4 studios to invest in better content, higher pay for performers, and to treat each performer with
5 respect and like an artist.

6 17. Unfortunately, Strike 3, like a large number of other producers of motion picture
7 and television works, has a major problem with Internet piracy. Often appearing among the
8 most infringed popular entertainment content on torrent websites, Strike 3’s motion pictures are
9 among the most pirated content in the world.

10 ***Defendant Used the BitTorrent File Distribution Network to Infringe Plaintiff’s Copyrights***

11 18. BitTorrent is a system designed to quickly distribute large files over the Internet.
12 Instead of downloading a file, such as a movie, from a single source, BitTorrent users are able
13 to connect to the computers of other BitTorrent users in order to simultaneously download and
14 upload pieces of the file from and to other users.

15 19. To use BitTorrent to download a movie, the user has to obtain a “torrent” file for
16 that movie, from a torrent website. The torrent file contains instructions for identifying the
17 Internet addresses of other BitTorrent users who have the movie, and for downloading the
18 movie from those users. Once a user downloads all of the pieces of that movie from the other
19 BitTorrent users, the movie is automatically reassembled into its original form, ready for
20 playing.

21 20. BitTorrent’s popularity stems from the ability of users to directly interact with
22 each other to distribute a large file without creating a heavy load on any individual source
23 computer and/or network. It enables Plaintiff’s motion pictures, which are often filmed in state
24 of the art 4kHD, to be transferred quickly and efficiently. Moreover, BitTorrent is designed so
25 that the more files a user offers for download to others, the faster the user’s own downloads
26 become. In this way, each user benefits from illegally distributing other’s content and violating

1 copyright laws.

2 21. Each piece of a BitTorrent file is assigned a unique cryptographic hash value.

3 22. The cryptographic hash value of the piece (“piece hash”) acts as that piece’s
4 unique digital fingerprint. Every digital file has one single possible cryptographic hash value
5 correlating to it. The BitTorrent protocol utilizes cryptographic hash values to ensure each
6 piece is properly routed amongst BitTorrent users as they engage in file sharing.

7 23. The entirety of the digital media file also has a unique cryptographic hash value
8 (“file hash”), which acts as a digital fingerprint identifying the digital media file (*e.g.*, a movie).
9 Once infringers finish downloading all the pieces which comprise a digital media file, the
10 BitTorrent software uses the file hash to determine that the file is complete and accurate.

11 ***Plaintiff’s Investigator Used a Tested and Accurate System to Identify Defendant’s***
12 ***Infringement***

13 24. Defendant used the BitTorrent file network to illegally download and distribute
14 Plaintiff’s copyrighted motion pictures.

15 25. Plaintiff’s investigator, IPP International U.G. (“IPP”) used a data collection
16 system titled “International IPTracker.” This system has been tested by experts who have
17 confirmed that it is not only accurate, but also superior to similar software law enforcement
18 uses.

19 26. The data collection system IPP used has a proprietary BitTorrent client which
20 enters into the swarm of infringers illegally infringing and distributing Plaintiff’s motion
21 pictures. A BitTorrent client is a program that allows a party to communicate with, and hence
22 download from, the BitTorrent swarm. The BitTorrent client is specialized—it does not seed or
23 distribute any of Plaintiff’s content. Additionally, neither Plaintiff, not its agents, upload any of
24 Plaintiff’s content to the BitTorrent network.

25 27. Once IPP’s BitTorrent client enters into the BitTorrent swarm, individual users
26 that are unlawfully sharing Plaintiff’s motion picture (like Defendant) connect to IPP’s

1 BitTorrent client and send IPP pieces of Plaintiff's motion picture.

2 28. In doing so, IPP's BitTorrent client establishes a direct TCP/IP connection with
3 the Defendant's IP address. The infringing transactions are recorded by IPP in the form of a
4 PCAP. PCAP stands for "packet capture" and it captures packets of information sent from one
5 computer to another computer over the Internet. As set forth in more detail below, discovery
6 will likely show that the IP address was not spoofed within a TCP/IP connection.

7 29. The PCAPs are stored on WORM tape drives. "WORM" stands for "write-once-
8 read-many." Once information is written onto a WORM tape drive, it cannot be altered.

9 30. International IPTracker uses a proprietary packet analyzer and TCPDump, an
10 open-source packet analyzer, to record the infringing transactions in PCAPs. TCPDump is
11 commonly used to accurately record network traffic.

12 31. The hardware used by IPP to log Defendant's IP addresses consists of a Hewlett
13 Packard BladeSystem c7000 Enclosure, 16x ProLiant BL460c G7 and 2x HP 1/10Gb-F VC-
14 Enet Module.

15 32. While Defendant was infringing, IPP downloaded from Defendant one or more
16 pieces of the digital media files containing Strike 3's motion pictures listed on Exhibit A
17 ("Works"). The transactions recorded in PCAPs, contain information about the .torrent file,
18 piece hash, BitTorrent client used by Defendant and time the transaction took place, among
19 other information.

20 33. The digital media files have been verified to contain a digital copy of a motion
21 picture that is identical (or alternatively, strikingly similar or substantially similar) to Plaintiff's
22 corresponding original copyrighted Works.

23 34. This process of recording the information in a PCAP is automatic and
24 inalterable. IPP then analyzes and confirms the information contained in these PCAPs. The
25 PCAP is a snapshot of the entire download as a whole and does not contain the completed and
26 viewable motion picture. The PCAP contains information about Defendant's download of the

1 motion picture over the BitTorrent network.

2 35. Each PCAP records Defendant's IP address transferring to IPP pieces of
3 Plaintiff's motion picture at the exact date and time that the transmission takes place.

4 36. The PCAP also records the pieces of Plaintiff's motion picture, along with the
5 cryptographic hash of that piece, which is unalterable.

6 37. In this way, the pieces of the movie recorded by IPP act as digital fingerprints.
7 Although the pieces of the movie may not be playable portions of Plaintiff's motion picture due
8 to technical reasons relating to video encoding techniques, each piece is forensic evidence of
9 Defendant's infringement in much the same way that fingerprints can identify a criminal
10 defendant at the crime scene. The fingerprints are identified by their SHA-1 hash value. *See*
11 *United States v. Dreyer*, 804 F.3d 1266, 1270 (9th Cir. 2015) (finding that similar law
12 enforcement technology "relies on unique file identifiers called SHA-1 hash values, which are
13 essentially 'digital fingerprint[s]' associated with electronic media. SHA-1 hash values remain
14 unchanged as long as the file itself is not altered").

15 38. Each PCAP contains two hashes that act as fingerprints. As set forth above, the
16 first hash identifies that Defendant was participating in the specific torrent swarm associated
17 with Plaintiff's motion pictures listed on Exhibit A. The second hash identifies the individual
18 piece that was transferred by Defendant, demonstrating that Defendant actually engaged in the
19 process of downloading and distributing Plaintiff's motion pictures.

20 39. Discovery will likely show that Defendant illegally downloaded and obtained a
21 full copy of Plaintiff's motion picture while simultaneously distributing the motion picture to
22 others. Indeed, IPP recorded Defendant distributing Plaintiff's motion pictures from May 2017
23 until December 2017. Defendant did not stop downloading and distributing Plaintiff's motion
24 pictures until after this lawsuit was filed.

25 40. The purpose of downloading and distributing Plaintiff's motion pictures is to
26 illegally obtain a full copy of the motion picture for viewing purposes.

1 41. Defendant downloaded and distributed 87 of Plaintiff's works over the
2 BitTorrent network to circumvent paying for them.

3 42. Plaintiff is unable to capture the full, or a playable portion of its motion picture
4 from Defendant because of the nature of the BitTorrent protocol. Because the BitTorrent
5 protocol is technically based on data exchange, a peer requires data to be uploaded (*i.e.*,
6 exchanged) to continue downloading. For that reason, it is very likely that a single peer quickly
7 refuses further downloads without receiving any uploads. Specifically, Plaintiff would likely
8 have had to share pieces of its own movie to Defendant, to receive a full copy, something which
9 Plaintiff does not do.

10 43. At no point was Plaintiff's copyrighted content uploaded by IPP to any
11 BitTorrent user. Further, Plaintiff does not upload any of its copyrighted works to the
12 BitTorrent network, nor does it authorize any of its agents to do so. Indeed, Plaintiff loses
13 revenue from real sales when people infringe its movies on the Internet.

14 ***Defendant's IP Address was Likely Not Spoofed, Used Without his Knowledge or Consent, or***
15 ***Otherwise Falsely Implicated***

16 44. It is extremely unlikely that Defendant's IP address was spoofed, used without
17 defendant's knowledge or consent, or otherwise falsely implicated because of the nature of how
18 IPP's software connects with Defendant. Indeed, discovery will likely show that Defendant is
19 the infringer, and not someone else.

20 45. A University of Washington Paper titled *Challenges and Directions for*
21 *Monitoring P2P File Sharing Networks – or – Why My Printer Received a DMCA Takedown*
22 *Notice* by Michael Piatek, Tadayoshi Kohno & Arvind Krishnamurthy, analyzes "the methods
23 by which copyright holders currently monitor the BitTorrent file sharing network," and
24 ultimately concludes that "a common approach for identifying infringing users is not
25 conclusive." See <http://dmca.cs.washington.edu>; see also *Malibu Media, LLC v. Doe*, No.
26 CV15-3504-JFB-SIL, 2016 WL 4444799, at *4 (E.D.N.Y. Aug. 23, 2016).

46. “In reaching their conclusion, the authors differentiate between ‘direct detection’ and ‘indirect detection’ of copyright infringers. *Id.* at § 2. Whereas direct detection ‘involves connecting to a peer . . . and then exchanging data with that peer,’ indirect detection ‘relies on the set of peers returned by the coordinating tracker [of a BitTorrent swarm] only, [and] treating this list as authoritative as to whether or not IPs are actually exchanging data within the swarm.’” *Id.* According to the authors, “[t]he main weakness in current methods of detecting copyright infringement in BitTorrent appears to be the treatment of *indirect reports* as conclusive evidence of participation.” *Id.* at § 4 (emphasis supplied). To that end, the authors note that “direct detection is more conclusive” *Id.* at § 2. Accordingly, the authors ultimately conclude that “[a] more thorough approach to detecting infringement in BitTorrent would be to . . . download data directly from the suspected user and verify its contents.” *Id.* at § 6.1.

47. Consistent with the findings in the University of Washington paper, IPP’s software utilizes a “direct detection method” to receive data directly with the seeder, thus ensuring the transaction data IPP records comes straight from the source (*i.e.*, the infringing IP address) and is not filtered through the swarm generally. As explained by Judge Locke: “By actually exchanging data with the seeder, [IPP] can be sure that person or that IP address has really shared that content” *Malibu Media, LLC v. Doe*, No. CV 15-3504-JFB-SIL, 2016 WL 4444799, at *5 (E.D.N.Y. Aug. 23, 2016) (internal punctuation and citation omitted).

48. This direct connection to the IP address prevents false-positives that may result from spoofing because there is, in effect, no middleman or straw transaction on which some superseding IP address could route IPP’s and Defendant’s connection.

49. Because the Court has not allowed Plaintiff the ability to view the subpoena response from Defendant’s ISP containing Defendant’s name and address, Plaintiff cannot, at this time, plead specific facts that would identify Defendant as the infringer, and not someone else, because Plaintiff does not know Defendant’s identity and therefore cannot conduct an

1 investigation.

2 50. However, discovery will likely show Defendant, and not someone else, used
3 BitTorrent to infringe Plaintiff's motion pictures because the protracted length and time of the
4 infringement—over six months—demonstrates that the infringer was someone with consistent
5 long-term access to Defendant's internet IP Address, *i.e.*, most likely the Defendant
6 himself/herself.

7 51. Moreover, discovery will likely show that Defendant is the infringer because, not
8 coincidentally, the infringement stopped once Plaintiff filed this lawsuit, indicating the
9 Defendant had control over his or her internet IP Address.

10 52. Defendant is a persistent and prolific infringer within the BitTorrent community
11 engaged in the unauthorized distribution of content owned and produced by members of the
12 MPAA, the BSA, the RIAA, and Microsoft during the months before Plaintiff filed this
13 lawsuit. After Plaintiff filed suit, the infringements emanating from Defendant's IP Address
14 ceased.

15 ***Plaintiff's Copyrights Are Registered with the United States Copyright Office***

16 53. Plaintiff owns the copyrights to the Works and the Works have been registered
17 with the United States Copyright Office. The United States Copyright Office registration
18 information for the Works, including the registration numbers, is outlined on Exhibit A. The
19 titles of these Works, date of publication, and other identifying information is accessible to the
20 public free of charge by searching the registration number in the Copyright Office's online
21 catalogue: <https://cocatalog.loc.gov/cgi-bin/Pwebrecon.cgi?DB=local&PAGE=First>. Plaintiff
22 can also provide a list of the specific titles under seal.

23 54. Plaintiff is entitled to seek statutory damages and attorneys' fees under 17 U.S.C.
24 § 501 of the United States Copyright Act.

Cause of Action

Direct Copyright Infringement

55. The allegations contained in paragraphs 1-54 are hereby re-alleged as if fully set forth herein.

56. Plaintiff is the owner of the Works, which are original works of authorship.

57. Defendant copied and distributed the constituent elements of Plaintiff's Works using the BitTorrent protocol.

58. At no point in time did Plaintiff authorize, permit or consent to Defendant's distribution of its Works, expressly or otherwise.

59. As a result of the foregoing, Defendant violated Plaintiff's exclusive right to:

(A) Reproduce its Works in copies, in violation of 17 U.S.C. §§ 106(1) and 501;

(B) Distribute copies of the Works to the public by sale or other transfer of ownership, or by rental, lease or lending, in violation of 17 U.S.C. §§ 106(3) and 501;

(C) Perform the copyrighted Works, in violation of 17 U.S.C. §§ 106(4) and 501, by showing the Works' images in any sequence and/or by making the sounds accompanying the Works' audible and transmitting said performance of the work, by means of a device or process, to members of the public capable of receiving the display (as set forth in 17 U.S.C. § 101's definitions of "perform" and "publically" perform); and

(D) Display the copyrighted Works, in violation of 17 U.S.C. §§ 106(5) and 501, by showing individual images of the works non-sequentially and transmitting said display of the works by means of a device or process to members of the public capable of receiving the display (as set forth in 17 U.S.C. § 101's definition of "publicly" display).

60. Defendant's infringements were committed "willfully" within the meaning of 17 U.S.C. § 504(c)(2).

Jury Demand

Pursuant to Fed. R. Civ. P. 38, Plaintiff respectfully demands a trial by jury of all issues so triable.

Prayer for Relief

WHEREFORE, Plaintiff respectfully requests that the Court:

(A) Permanently enjoin Defendant from continuing to infringe Plaintiff's copyrighted Works;

(B) Order that Defendant delete and permanently remove the digital media files relating to Plaintiff's Works from each of the computers under Defendant's possession, custody or control;

(C) Order that Defendant delete and permanently remove the infringing copies of the Works Defendant has on computers under Defendant's possession, custody or control;

(D) Award Plaintiff statutory damages per infringed work pursuant to 17 U.S.C. § 504(a) and (c);

(E) Award Plaintiff its reasonable attorneys' fees and costs pursuant to 17 U.S.C. § 505; and

(F) Grant Plaintiff any other and further relief this Court deems just and proper.

DATED this 3rd day of July, 2018

FOX ROTHSCHILD LLP

s/ Bryan J. Case
Bryan J. Case, WSBA #41781
Lincoln D. Bandlow, *admitted Pro Hac Vice*
(CSBA #170449)

Attorneys for Plaintiff

FIRST AMENDED COMPLAINT
(Case No.: 2:17-cv-01731-TSZ)

FOX ROTHSCHILD LLP
1001 Fourth Avenue, Suite 4500
Seattle, WA 98154
(206) 624-3600

CERTIFICATE OF SERVICE

I hereby certify that on July 3, 2018, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the following persons:

J. Curtis Edmondson, WSBA #43795	<input checked="" type="checkbox"/>	Via CM/ECF
399 NE John Olsen Avenue	<input type="checkbox"/>	Via U.S. Mail
Hillsboro, Oregon 97124	<input type="checkbox"/>	Via Messenger Delivery
Telephone: (503) 336-3749	<input type="checkbox"/>	Via Overnight Courier
Email: jcedmondson@edmolaw.com	<input type="checkbox"/>	Via Facsimile

DATED this 3rd day of July, 2018.

/s/ Christine F. Zea
Christine F. Zea
Floating Legal Administrative Assistant

FIRST AMENDED COMPLAINT
(Case No.: 2:17-cv-01731-TSZ)

FOX ROTHSCHILD LLP
1001 Fourth Avenue, Suite 4500
Seattle, WA 98154
(206) 624-3600